ma
the
ma
tisch

cen
trum

MC

AFDELING ZUIVERE WISKUNDE
(DEPARTMENT OF PURE MATHEMATICS)

ZN 91/79 JUNI

A.E. BROUWER

A FEW NEW CONSTANT WEIGHT CODES

amsterdam 1979

stichting
mathematisch
centrum

MC

AFDELING ZUIVERE WISKUNDE
(DEPARTMENT OF PURE MATHEMATICS)

ZN 91/79 JUNI

A.E. BROUWER

A FEW NEW CONSTANT WEIGHT CODES

2e boerhaavestraat 49 amsterdam

Printed at the Mathematical Centre, 49, 2e Boerhaavestraat, Amsterdam.

The Mathematical Centre, founded the 11-th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O).

AMS(MOS) Subject classification scheme (1970): 05B40, 94B25

A few new constant weight codes

by

A.E. Brouwer

ABSTRACT

We describe a method for searching for constant weight codes and show its usefulness by constructing fourteen codes which are better than the known codes with the same parameters.

KEY WORDS & PHRASES: *constant weight codes.*

Let G be a permutation group of degree n acting on a set X, say $\{0,1,\ldots,n-1\}$. A code C is called G-invariant if whenever $(c_0,c_1,\ldots,c_{n-1}) \in C$ and $g \in G$, then also $(c_{g(0)},c_{g(1)},\ldots,c_{g(n-1)}) \in C$.

$\mathbb{Z}_n$-invariant codes are known as cyclic codes and have received a good deal of attention. Recently R.E. Kibler found some good G_n-invariant codes for $G_n = \{x \mapsto ax+b \pmod n \mid 0 \le a,b \le n-1,\ (a,n) = 1\}$ acting on the ring of residues mod n. This gave me the idea for this note.

Let us first translate the problem: An (n,d,w)-code is a binary code with word length n, minimum distance d and constant weight w. A(n,d,w) is the maximum cardinality of such a code. (Note that d is even.) Now any (n,d,w)-code can be considered as a collection of w-subsets of an n-set such that no two w-subsets have a $(w-\frac{1}{2}d+1)$-set in common. Searching for (n,d,w)-codes is thus seen to be the same as looking for good approximations to t-(v,k,1) designs, where v = n, k = w and $t = w-\frac{1}{2}d+1$. For certain values of the parameters this is done most conveniently by a modification of Kramer & Mesner's method: Referring to their paper [3] we can copy all of their machinery and replace their equation

$$A\bar{x} = \lambda[1\,1\,\ldots\,1]^T \quad ((1),\ p.265) \quad \text{by} \quad A\bar{x} \le [1\,1\,\ldots\,1]^T.$$

Now all that remains to do is thinking of a nice group and waiting for the computer output (the process is rather efficient - I did the research for this note sitting behind my terminal for one evening; surely many more codes may be found in the same way).

Some examples:

- Let $X = \mathbb{F}_{13} \cup \{\infty\}$ and $G = GA_{13} = \{x \mapsto ax+b \mid a,b \in \mathbb{F}_{13},\ a \neq 0\}$ acting on X in the obvious way.
  We find a G-invariant (14,4,5)-code of size 169, showing that $A(14,4,5) \ge 169$.
  (Note that Kibler showed that the best cyclic code with these parameters has size 154.)
- Let $X = \mathbb{F}_7 \times \{0,1\}$ and $G = GA_7$ acting on X in the obvious way.
  We find a very nice G-invariant (14,4,7)-code, showing that $A(14,4,7) \ge 316$. (Kibler found $A(14,4,7) \ge 254$.)

Fixing one coordinate produces a (13,4,6)-code of size 158. (Note that Kibler showed that the best cyclic code with these parameters has size 156.) There are 13 ways of shortening this last code; one produces a code of 66, six produce a code of size 73 and six produce a code of size 74. Hence $A(12,4,5) \geq 74$. (Shen Lin found $A(12,4,5) \geq 73$.)

- Let $X = \mathbb{F}_9 \times \{0,1\}$ and $G = GA_9$ acting on X in the obvious way. We find $A(18,4,5) \geq 504$.
- Let $X = PG(1,6) \times \{0,1\}$, two copies of the projective line over $\mathbb{F}_7$, and G the group PGL(2,7) of order $6 \cdot 7 \cdot 8 = 336$ acting on both lines simultaneously. We find $A(16,4,8) \geq 1122$, so that $A(15,4,7) \geq 561$. (But see below.)
- Let $X = PG(1,8) \times \{0,1\}$ and $G = PGL(2,8)$ of order $7 \cdot 8 \cdot 9 = 504$ acting in the obvious way. We find $A(18,4,6) \geq 1260$ and hence $A(17,4,6) \geq 840$.
- Let $X = \mathbb{F}_{16}$ and $G = \{x \mapsto ax+b \mid a,b \in \mathbb{F}_{16}, a^5 = 1\}$ of order 80. We find $A(16,4,6) \geq 592$ and shortening yields $A(15,4,5) \geq 222$.
- Let $X = \mathbb{F}_{16}^*$ and $G = \{x \mapsto ax^{2^i} \mid a \in \mathbb{F}_{16}^*, i = 0,1,2,3\}$ of order 60. We find $A(15,4,6) \geq 370$.
- Let $X = PG(1,7) \times \{0,1\}$ and $G = PSL(2,7)$ of order $336/2 = 168$. This gives even better results than PGL(2,7) above. We find $A(16,4,8) \geq 1164$, so that $A(15,4,7) \geq 582$. This (16,1164,4,8) code can be shortened in several inequivalent ways. If I'm not mistaken the best results obtainable in this way are $A(14,4,6) \geq 275$, $A(14,4,7) \geq 314$ (but above we found $A(14,4,7) \geq 316$), $A(13,4,5) \geq 118$, $A(13,4,6) \geq 158$, $A(12,4,4) \geq 48$ (but $A(12,4,4) = 51$ is well known), $A(12,4,5) \geq 75$. Thus, even after shortening it four times, this code produces improvements on the known bounds!

REFERENCES

[1] BEST, M.R., A.E. BROUWER, F.J. MacWILLIAMS, A.M. ODLYZKO & N.J.A. SLOANE, *Bounds for binary codes of length less than* 25, IEEE Trans. on Inf. Theory, IT-24 (1978) 81-93.

[2] KIBLER, R.E., *Improved lower bounds for some values of* A(n,d,w), preprint, 1979.

[3] KRAMER, E.S. & D.M. MESNER, *t-designs on hypergraphs,* Discrete Math. 15 (1976), 263-296.

Egeldonk, 790613